UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/533,120	09/19/2005	Bernard Smeets	2380-889	7035

23117 7590 02/12/2009

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
02/12/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/533,120	SMEETS ET AL.	
	Examiner	Art Unit	
	MICHAEL PYZOCHA	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 April 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *47-75* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *47-75* is/are rejected.

7)☒ Claim(s) *65* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 April 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *9/19/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 47-75 are pending.

2. Preliminary amendment filed 04/29/2005 has been received and considered.

Claim Objections

3. Claim 65 is objected to because of the following informalities: in the third line of claim 65 the numeral "20" is present when it has no need. Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 52-54 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: the claims state that the trigger data is generated based on the stored secret and the configurational device-specific security data; however, the trigger data is on based off of a cryptographic representation of the configurational device-specific security data and the stored secret is never used even though it is required by the claim.

6. Any claims not specifically addressed are rejected by virtue of their dependencies.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 47, 48, 51-54, 58-64, 66, 67, 69-71, 73 and 75 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hopkins et al. (EP 1081891) in view of Challener et al. (US 6470454).

As per claims 47, 66 and 70, Hopkins et al. discloses means for tamper-resistantly storing a secret not accessible over an external circuit interface (see paragraph [0032]); means for performing processing at least partly in response to said stored secret to generate an instance of device-specific security data internally confined within said electronic circuit during usage of said device; and means for performing a security-related operation in response to said internally confined device-specific security data (see paragraph [0039]).

Hopkins et al. fails to explicitly disclose that the device-specific security data is generated by performing cryptographic processing on at least partially the stored secret.

However, Challener et al. teaches performing cryptographic processing on at least partially secret data to create device-specific security data (see abstract and column 5 lines 28-50).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to create the device information of Hopkins et al. using a cryptographic hash.

Motivation to do so would have been to allow a user to create device specific information (see Challener et al. column 5 lines 28-50).

As per claims 48, 67 and 71 the modified Hopkins et al. and Challener et al. system discloses said device is a network device and said operation is related to at least one of data confidentiality, data integrity, authentication, authorization and non-repudiation in network communication (see Hopkins et al. paragraphs [0030] through [0032]).

As per claims 51-54, 69, 73 and 75, the modified Hopkins et al. and Challener et al. system discloses creating an using triggering data based from cryptographic functions (see Challener column 5 lines 28-50 and Hopkins et al. paragraphs [0046] through [0053]).

As per claims 58-61, the modified Hopkins et al. and Challener et al. system discloses performing additional cryptographic processing based on device-specific security data and external data to generate further security data and performing security-related operations in response to said security data where the system is configured to generate and use certain encryption keys (see Hopkins et al. paragraphs [0046] through [0053]).

As per claims 62-64 the modified Hopkins et al. and Challener et al. system discloses generating a private key based at least partially on said stored secret (see

Hopkins et al. paragraph [0039] as combined with Challener et al. column 5 lines 28-50) and using the private key and corresponding public key to generate a shared key (see Hopkins et al. paragraphs [0046] through [0053]).

9. Claims 49, 50, 68 and 72 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Hopkins et al. and Challener et al. system as applied to claims 47, 66 and 70 above, and further in view of Venkatesan et al. (US 20040001605).

As per claims 49, 50, 68 and 72, the modified Hopkins et al. and Challener et al. system fails to explicitly disclose that the device is configured for producing digital content by marking (by embedding a fingerprint in) said digital content based on the device-specific security data.

However, Venkatesan et al. teaches marking produced content with specific security information (see paragraph [0053]).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the device specific security information of the modified Hopkins et al. and Challener et al. system to watermark produced content.

Motivation to do so would have been to uniquely identify the content as original (see Venkatesan et al. paragraph [0053]).

10. Claims 55-57 and 74 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Hopkins et al. and Challener et al. system as applied to claims 47 and 73 above, and further in view of Beatson (US 20030056100).

As per claims 55-57 and 74, the modified Hopkins et al. and Challener et al. system disclose authenticating a manufacturer and providing information to the manufacturer (see Hopkins paragraphs [0039] through [0042]), but fails to disclose allowing/preventing access to the security information based on an access code.

However, Beatson teaches and access code to prevent/allow access to a device (see Beatson paragraph [0084]).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to require an access code to use the device of the modified Hopkins et al. and Challener et al. system.

Motivation, as recognized by one of ordinary skill in the art, to do so would have been to prevent unauthorized access to the security data.

11. Claim 65 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Hopkins et al. and Challener et al. system as applied to claim 47 above, in view of Xiao et al. (WO 0077974) and further in view of Matyas, Jr. et al. (US 6687375).

As per claim 65, the modified Hopkins et al. and Challener et al. system fails to disclose generating a chain of keys by hashing a previous key with an identity.

However, Xiao et al. teaches chaining based off values of keys (see page 9 lines 1-10) and Matyas, Jr. et al. teaches creating a key by hashing a key with identity information (see FIG. 4 and column 9 lines 3-17).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to create a chain of user dependent keys in the modified Hopkins et al. and Challener et al. system.

Motivation to do so would have been to create a chain of trust (see Xiao et al. page 9) and to create a user specific key (see Matyas, Jr. et al. column 9 lines 3-17).

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The remaining references cited on the PTO-892 are directed to security related devices and are relevant to the claimed invention.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL PYZOCHA whose telephone number is (571)272-3875. The examiner can normally be reached on Monday-Thursday, 7:00am - 4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Michael Pyzocha/
Examiner, Art Unit 2437